Appendix D

RELIABILITY

MIL-STD-721C, Subj: Definitions of Terms for Reliability and Maintainability, provides two definitions for reliability:

1. The duration of probability of failure-free performance under stated conditions.

2. The probability that an item can perform its intended function for a specified interval under stated conditions. (For non-redundant items, this is equivalent to definition 1. For redundant items this is equivalent to definition of mission reliability).

In order to be capable of measuring the A_o of a system under development, the Program Manager must be capable of assessing system reliability both quantitatively and qualitatively. Quantitative assessment of reliability requires knowledge of system and equipment failure frequency, expressed as Mean Time Between Failure (MTBF). Qualitative assessment of system reliability requires the Program Manager to understand the system's probable failure modes, effect of failures on the mission, and the design engineering effort required to eliminate unacceptable failure modes. A_o is established through a combination of the reliability and maintainability design characteristics of subsystems, equipments and the support system design. It is essential that the program Manager is capable of accurately assessing system reliability during the design phase when the reliability elements of A_o are established. A_o of a system can never exceed the inherent design reliability of the equipment no matter how good the production, quality or maintenance program may be. The design disciplines and analyses that are discussed in this section are intended to identify and focus attention on equipment design weaknesses so that they may be corrected, protected against, or accepted after consideration in A_o trade-off analyses. They also provide a means of assuring that a design will meet specified MTBF (reliability) requirements prior to test or production commitments. This approach is known as "Reliability by Design".

Reliability by Design The Reliability by Design approach differs in several key areas from traditional reliability programs. The emphasis is on making reliability an integral part of the design process rather than something done by a group of reliability experts separate from the designers. The objective is to get designers to consider those factors which affect component life with the same emphasis as those factors which affect system performance. Accomplishing this objective entails the translation of operational reliability requirements into meaningful design requirements. The Reliability by Design approach differs in another major way from the traditional reliability approach. Since the emphasis is on the design itself, there is a resulting de-emphasis on program plans and formal reliability demonstration testing. There is a greater payoff in spending more time and resources on performing the design process than on testing the design to determine if it complies with requirements. There is a very sound basis for this reasoning. First, there are analytical techniques which allow assessment of reliability before hardware buildup, when changes can be easily instituted. Second, as reliability requirements increase in magnitude, the practicality of demonstrating them through testing diminishes because of extremely long and costly test times required to do so. For instance, it would take over 11,000 hours of test time to demonstrate a 5,000 hour MTBF with 90% confidence under optimum conditions (zero failures). The impact on program schedules, coupled with the expense of corrective action late in system development when hardware is available for test, may make reliability demonstrations infeasible.

MIL-STD-785B, establishes the various tasks which are required in a basic reliability engineering program. Figure D-l presents a matrix of the various tasks in MIL-STD-785B.

The level of confidence that a Program Manager has in his/her ability to assess design reliability, and also in the data derived in the assessment, depends directly on his level of understanding of the reliability by design process. Therefore, this section will briefly describe some basic tools of the process; concentrating on establishing reliability requirements (allocation); assessing the inherent design reliability (prediction); and the identification and correction of design weaknesses (Failure Mode, Effects and Criticality Analysis (FMECA)). The first step in performing all of these analyses is development of a design reliability model. Because design reliability assessment is properly performed early in the system design process, the Program Manager does not yet have a system available to perform the analysis. Therefore, he must create a realistic model of the system which may be exercised for reliability allocation, prediction and design analysis.

RELIABILITY MODELING

Objectives of a Model Reliability modeling is an integral part of almost all reliability program plans. As pointed out in MIL-STD-785B, a reliability model of the system or equipment is required for making numerical apportionments and estimates of reliability. A system model is mandatory for evaluating complex series-parallel equipment arrangements which usually exist in military systems. In accordance with requirements of MIL-STD-756B, it is common practice to define a Basic Reliability Model and a Mission Reliability Model.

The Basic Reliability Model is a series model used for estimating the demand for maintenance and logistic support caused by the system and its component parts. In the Basic Reliability Model, all elements of the system, even those provided for by redundancy, or alternate modes of operation, are modeled in series. In other words, the Basic Reliability Model consists of a reliability block diagram, with all the blocks in series, and an associated mathematical expression which relates failure rate, duty cycle, and mission duration data to failures in the series of elements.

The Mission Reliability Model, on the other hand, consists of a reliability block diagram and associated mathematical description that depicts the intended utilization of the system to achieve mission success. Elements of the system, provided for by redundancy or alternate modes of operation, are shown in the reliability block diagram in a parallel configuration appropriate to the mission phase or mission application.

Reliability modeling efforts are useful at all stages in system development. In early development stages, they are needed to translate operational requirements for the system into a set of meaningful reliability requirements for each component through the allocation process. In later stages of development, as the design progresses, the modeling efforts are useful in assessing the degree to which the system reliability requirements are being met. Modeling efforts are also useful in the evaluation of alternative design approaches to achieve system functions. The model may be useful in evaluating the effects of proposed changes to the system, even after production and deployment.

TASK NUMBER	TITLE	TASK TYPE	PROGRAM PHASE			
			CON-CEPT	D+V	FSD	PROD
101	Reliability program plan	MGT	S	S	G	G
102	Monitor/control of subcontractors and suppliers	MGT	S	S	G	G
103	Program reviews	MGT	S	S(2)	G(2)	G(2)
104	Failure reporting, analysis, and corrective action system (FRACAS)	ENG	NA	S	G	G
105	Failure review board (FRB)	MGT	NA	G	G	G
201	Reliability modeling	ENG	S	S(2)	G(2)	GC(2)
202	Reliability allocations	ACC	S	G	G	GC
203	Reliability predictions	ACC	S	S(2)	G(2)	GC(2)
204	Failure modes, effects, and criticality analysis (FMECA)	ENG	S	S(1) (2)	G(1) (2)	GC(1) (2)
205	Sneak circuit analysis (SCA)	ENG	NA	NA	G(1)	GC(1)
206	Electronic parts/circuits tolerance analysis	ENG	NA	NA	G	GC
207	Parts program	ENG	S	S(2) (3)	G(2)	G(2)
208	Reliability critical items	MGT	S(1)	S(1)	G	G
209	Effects of functional testing, storage, handling, packaging, transportation, and maintenance	ENG	NA	S(1)	G	GC
301	Environmental stress screening (ESS)	ENG	NA	S	G	G
302	Reliability development/growth testing	ENG	NA	S(2)	G(2)	NA
303	Reliability qualification test (RQT) program	ACC	NA	S(2)	G(2)	G(2)
304	Production reliability acceptance test (PRAT) program	ACC	NA	NA	S	G(2) (3)

CODE DEFINITIONS:

TASK TYPE

ACC - Maintainability accounting
ENG - Maintainability engineering
MGT - Management

PROGRAM PHASE

S - Selectively applicable
G - Generally applicable
GC - Generally applicable to design changes only
NA - Not applicable

(1) Requires considerable interpretation of intent to be cost effective

(2) MIL-STD-785 is not the primary implementation requirement. Other MIL-STDs or statement of work requirements must be included to define the requirements.

Figure D-1: Reliability Task Application Matrix

The basic information for a reliability model is derived from functional or schematic descriptions of the system that depict the relationship or system components. The reliability model reorients the diagrams into a series/parallel network of blocks (a reliability block diagram) showing the reliability relationships among the various components of the system. These diagrams together with the appropriate duty cycle, mission duration, and component failure rate data are used to develop mathematical expressions that provide estimates of mission reliability.

Application of the Reliability Model Figure D-2 illustrates the process by which a reliability modeling effort may be used to generate a set of reliability requirements for components to achieve the operational reliability requirement for the system. The basic reliability model is developed by the application of expected component failure rates to the reliability block diagram. Examples of reliability block diagrams are presented in Figures D-3 and D-4. An estimate of system reliability is derived by mathematical computation of the reliability model, either through a manual process for simple systems, or computer simulation.

In the early phases of system development, the specific equipments may not yet be selected or designed. Specific failure rates cannot be established at this time. However, reliability assessment can be accomplished by assuming the failure rates of equipments in existing systems with similar functions.

Basic Mathematics of a Reliability Model The reliability of an item is generally expressed as the probability that the item will satisfactorily perform its intended function for a given period of time under specified conditions of use. Therefore, a model of system reliability characteristics must reflect the system design and operating characteristics. The detailed mathematical model which is constructed to serve as the basis of allocation, prediction, and engineering must relate reliability to design configuration, modes of operation, duty cycles, and use conditions.

Mathematical expressions for simple cases represented by series of parallel elements and series-parallel functional relationships are utilized as building blocks to build a model to the equipment or system level. Figure D-5 illustrates the process. The level of detail in a reliability model depends on the stage of system development and the level of detail available on the system and equipment design.

Two important mathematical parameters in a reliability model are: units of measure of reliability, and the independence of failure events. Units of measure for reliability depend on system/equipment utilization. The equipment involved in a system usually can be broken down into three major categories determined by their mode of operation: continuous, intermittent, and impulse operations. The reliability of continuous-use equipment, such as computers and radar or electronic equipment, is defined in terms of the reliability parameter of failures per unit time or MTBF. The reliability of intermittent-use equipment, such as magazines or load and launch equipment, is defined in terms of the reliability parameter of failures per cycle. Impulse operations, or go/no-go events, where time of operation is very short, as in fuse or squib operations, are defined by the number of successes per number of attempts.

The mathematics applied in the relatively simple models presented in this Appendix are based on assumptions of statistical independence between the elements of the system described in reliability block diagrams. Failure of one component of the system is assumed to be independent of failures of other components. It is not necessary in modeling or allocation mathematics for independence to exist, but the mathematics become increasingly difficult if independence of failure events is not assumed. Although the simplification of assuming independence of failure events may not apply to all equipments, most reliability

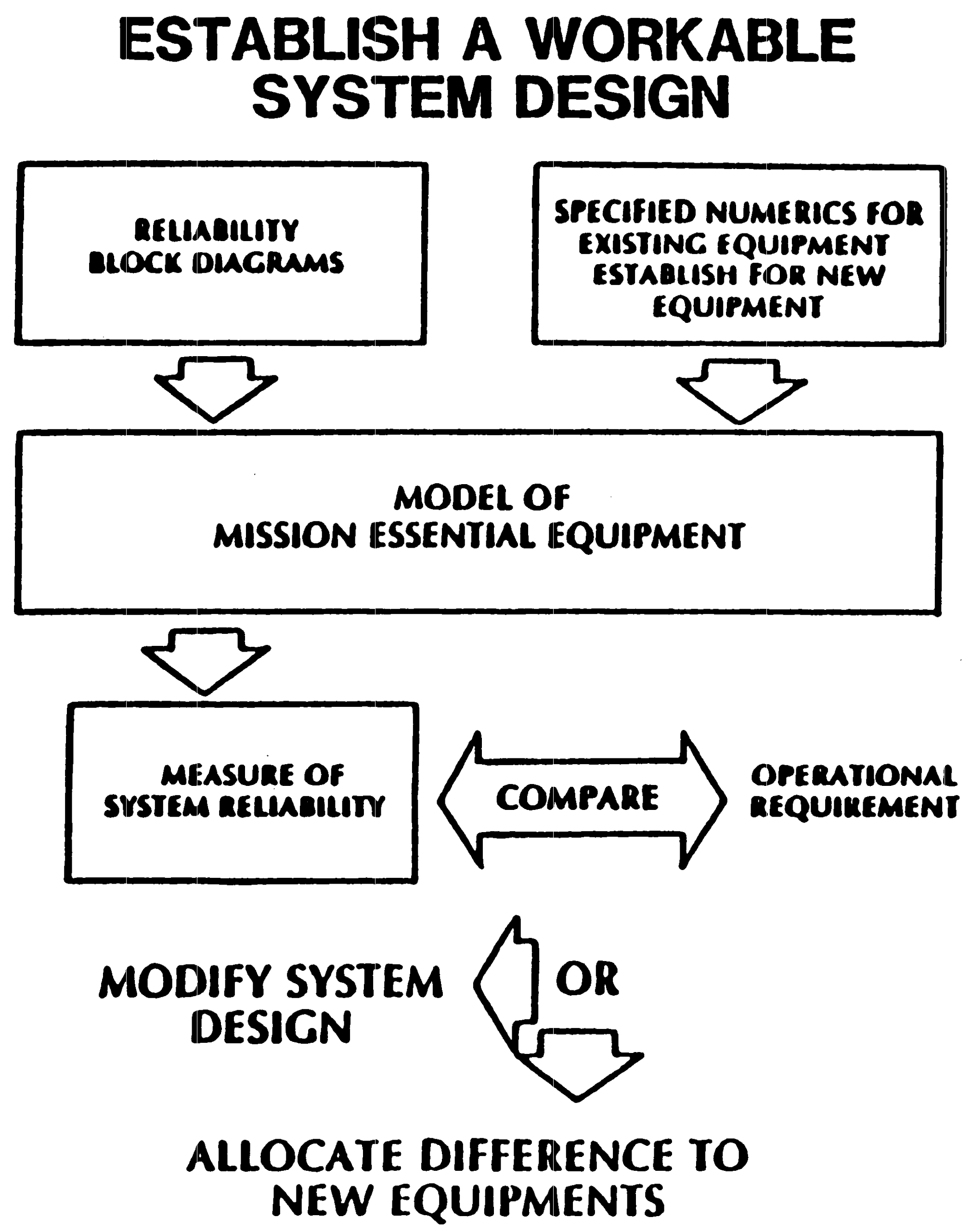
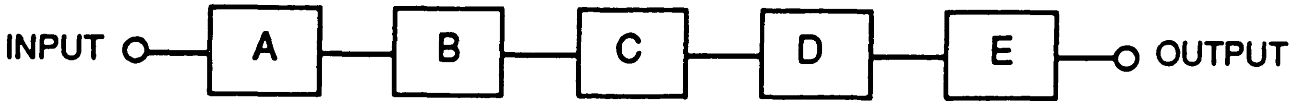

ESTABLISH A WORKABLE SYSTEM DESIGN
RELIABILITY BLOCK DIAGRAMS
SPECIFIED NUMERICS FOR EXISTING EQUIPMENT ESTABLISH FOR NEW EQUIPMENT
MODEL OF MISSION ESSENTIAL EQUIPMENT
MEASURE OF SYSTEM RELIABILITY
COMPARE
OPERATIONAL REQUIREMENT
MODIFY SYSTEM DESIGN
OR
ALLOCATE DIFFERENCE TO NEW EQUIPMENTS

Figure D-2: The Reliability By Design Process

Figure D-2

EXAMPLES OF A SERIES BLOCK DIAGRAM



R is the reliability of the input/output system

$R_{series} = P_A P_B P_C P_D P_E$

(If all elements are identical)

$R = p^n$ n = number of elements

1. Problem
   a. $P_A = P_B = P_C = P_D = P_E = 0.98$
   b. What is the system reliability?
   c. Answer: $R = p^n = (0.98)^5 = 0.9039$

λ is the failure rate of the input/output system

$\lambda_{series} = \lambda_A + \lambda_B + \lambda_C + \lambda_D + \lambda_E$

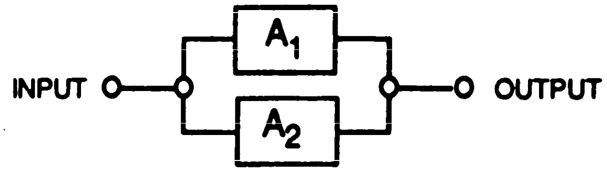
(If all elements are identical)

$\lambda_{series} = n \times \lambda$; n = number of elements

2. Problem
   a. $\lambda_A = \lambda_B = \lambda_C = \lambda_D = \lambda_E = 0.02$
   b. What is the system failure rate?
   c. Answer: $\lambda_{series} = n \times \lambda = 5 \times 0.02 = 0.1$

Figure D-3

EXAMPLES OF A PARALLEL RELIABILITY BLOCK DIAGRAM



R parallel $= P_1 + P_2 - P_1 P_2$

1. Problem

a. $P_1 = P_2 = 0.90$

b. What is the system reliability?

c. Answer: $R = P_1 + P_2 - P_1 P_2 = 0.90 + 0.90 - 0.81 = 0.99$

NOTE:

(1) N parallel elements

(2) All identical

(3) $R = 1 - q^n$ where q = unreliability or 1 - R

$R = 1 - (1-R)^n$

(4) Above Example:

$R = 1 - (1 - 0.9)^2 = 0.99$

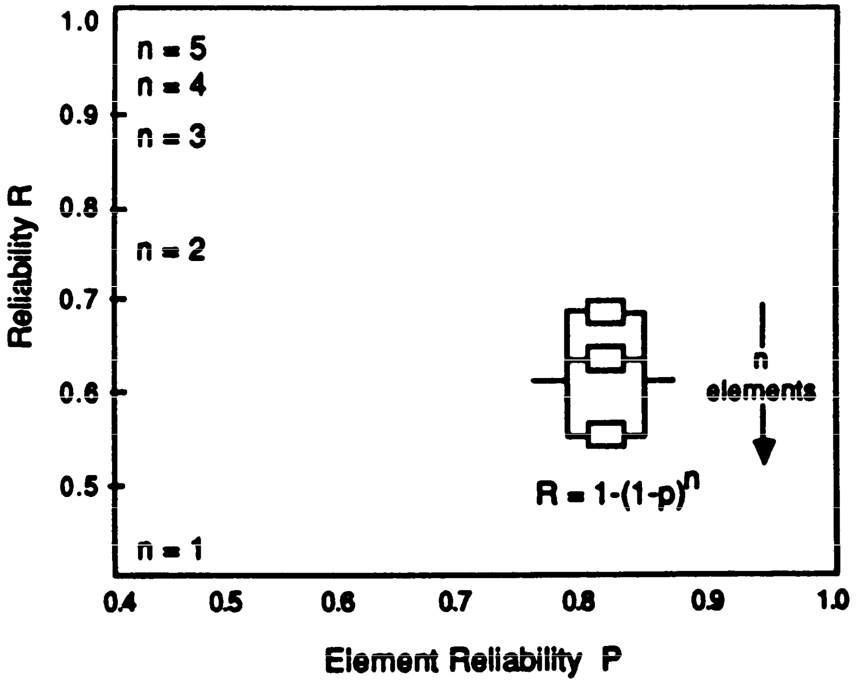


Figure D-4

LEVELS OF INDENTURE IN BLOCK DIAGRAMS

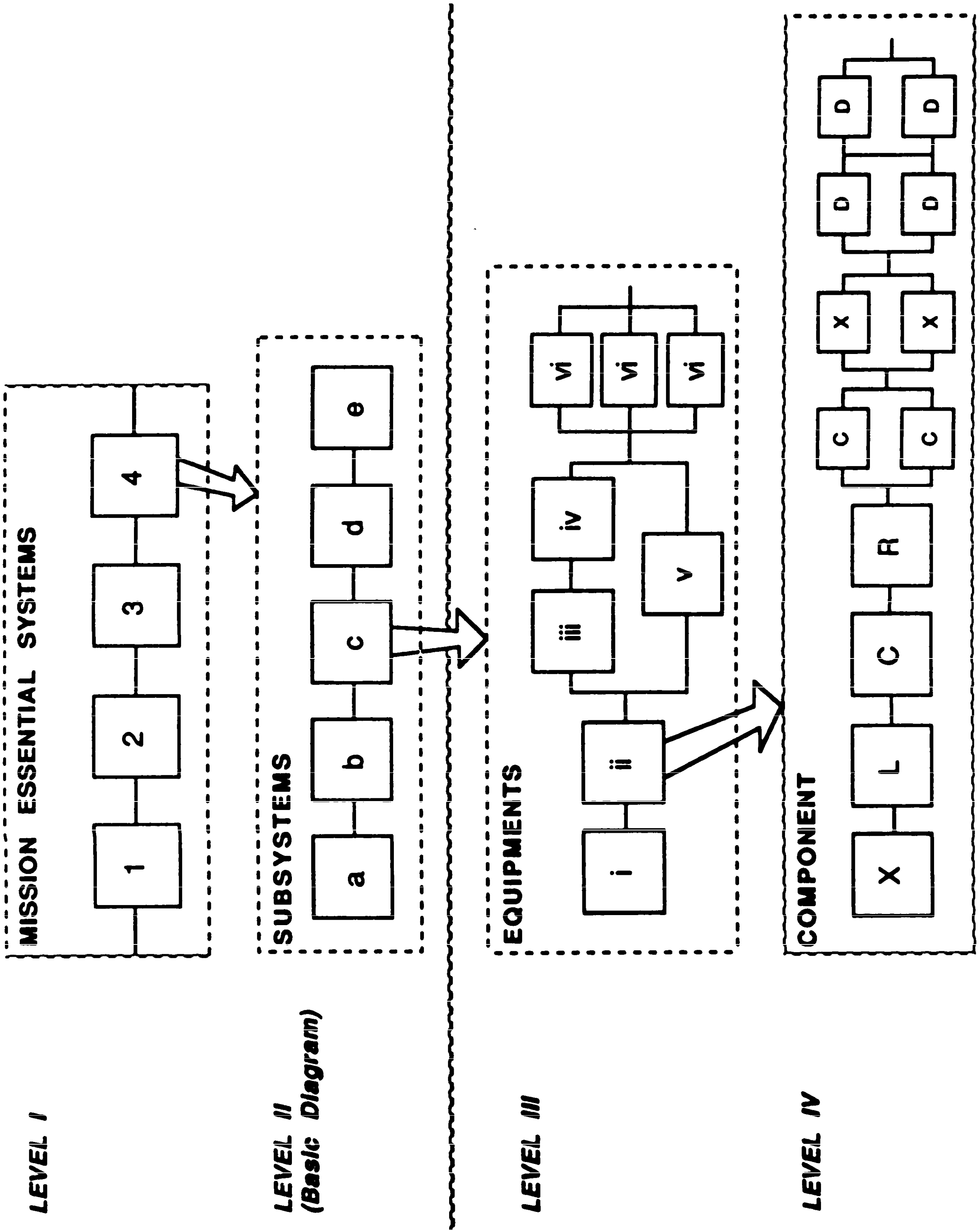


Figure D-5: Levels of Indenture in Block Diagrams

606-057

Figure D-5

math models are built on this assumption. Independence of failures is generally true for electronic components, but may not be true for mechanical failures. For example, the failure of a lube oil pump may cause a bearing to overheat and become a secondary failure.

RELIABILITY ALLOCATION

Objective of the Allocation After the reliability model is established and functional relationships are defined, the Program Manager is able to determine the reliability values required of each subsystem in order to achieve the level of system reliability demanded by the A_o objectives. This process is reliability allocation.

Reliability allocation represents the assignment of reliability thresholds to subsystems in such a manner that the system reliability requirements will be satisfied. Allocation employs the reliability model by proceeding from system reliability requirements to compatible subsystem thresholds. Allocated reliability requirements are useful in directing reliability effort along profitable channels, and for compatibility among the various development efforts. A few important uses of reliability allocation are listed below:

- During the conceptual phase, allocation of proposed reliability requirements aids in the determination of technical feasibility

- When various subsystems are developed by different contractors, allocation provides compatible contractual reliability requirements

- Allocation provides the prime contractor, as well as government monitors, with a means of evaluating subcontractor reliability achievements

- Allocated reliability requirements may be used as developmental goals for parts and subsystems. Reliability growth progress can be monitored for subsystems to avert problem areas, reallocate resources and efforts, or initiate appropriate reliability trade-offs.

When the allocation is combined in consonance with the reliability model, the allocated thresholds must yield a system reliability which is not less than the requirements specified in the system specification. The resulting reliability goals provide the basis for establishing comparisons of requirements with predictions. Such comparisons serve as a measure for detecting potential problem areas for adjusting the reliability thresholds. The allocation process is an approximation. The reliability parameters apportioned to the subsystems are used as guidelines to determine design feasibility. If the allocated reliability for a specific subsystem cannot be achieved at the current state of technology, the system design must be modified and the reliability of the subsystems reallocated. This procedure is repeated until an allocation is achieved that satisfies the system level requirements, accommodates all constraints, and results in subsystems that can be designed within the current or achievable technology.

If it is found that even with reallocation some of the individual subsystem requirements cannot be met with current technology, the designer may use one or any number of the following approaches (assuming that they are not mutually exclusive) in order to achieve the desired reliability:

- find a more reliable design or use more reliable component parts

- simplify the design by using fewer component parts if this is possible without degrading performance
- apply component derating techniques to reduce the estimated failure rates
- use graceful degradation or redundancy for those cases in which (1), (2), and (3) cannot produce the desired reliability; and
- reassess the Baseline Operational Scenario and Tentative Operational Requirement (TOR).

Practical Considerations in Reliability Allocation The ideal apportionment would allocate reliability design requirements to achieve the most economical use of resources, including time and cost. Allocation of reliability is a trade-off between the reliabilities of the system's individual components to achieve a specified total system reliability. By imposing high requirements on those units in which reliability is easier to attain, and lower requirements in those more difficult and more costly areas, the overall cost of system development may be controlled. A few important factors for consideration are:

- The complexity of the system will have an effect on the achievable reliability. The more complex the system, the greater the number of subassemblies and modules, and the more difficult and costly it is to achieve a high reliability. Imposing an unrealistically high reliability on a more complex system increases the cost disproportionately when compared with the effect of increasing the reliability requirement for a simpler system.
- The amount of development and research required to produce the system will greatly influence the time and cost of development. Imposition of a high reliability requirement on a system under development will increase the development time, the length of tests required to demonstrate the reliability, and the overall cost.
- The intended operational environment will determine the achievable reliability. A system to be used in a rugged environment will cost more to develop than a similar one to be used under less severe conditions with an equal reliability.
- The mission's length and time the equipment is required to perform influences the achievable reliability. It requires more development effort. It costs more to produce a system capable of operating for a long time without failure than to develop one for a shorter period of use.
- A component's high reliability is based on the importance of its operation. A component whose failure would not jeopardize the accomplishment of the mission, need not be highly reliable. To the extent that failures can be tolerated, lower reliability requirements may be imposed.

Reliability Allocation Methods There are a number of approaches to allocating reliability requirements. Two of these are designated as the Equal, or Fair share, allocation method and the other is allocation by complexity, or the Weighted Allocation method.

Equal Allocation Method In the absence of definitive information of the system, other than the fact that n subsystems are to be used in series, equal allocation to each subsystem is reasonable. In this case, the n^{th} root of the system reliability requirement would be allocated to each of the n subsystems.

The equal allocation technique assumes a series of n subsystems, each of which is assigned the same reliability threshold. A prime weakness of the method is that the subsystem thresholds are not assigned in accordance with the degree of difficulty associated with achievement of these requirements. For this technique the model is:

$$R_S = \prod_{i=1}^{n} R_i$$

or

$$R_i = (R_S)^{1/n} \text{ for } i = 1,2,\ldots,n$$

Where: R_S is the required system reliability
R_i is the reliability requirement apportioned to subsystem i

Example: Consider a proposed communication system which consists of three subsystems (transmitter, receiver, and coder), each of which must function if the system is to operate. Each subsystem is developed independently. Assuming each is equally expensive to develop, what reliability requirement should be assigned to each subsystem in order to meet a system requirement of 0.729?

The apportioned subsystem requirements are found as:

$$R_T = R_R = R_C = (R_S)^{1/M} = (0.729)^{1/3} = 0.90$$

Thus a reliability requirement of 0.90 would be assigned to each subsystem.

Allocation by Complexity This method assumes series subsystems with constant failure rates in a series, such that any subsystem failure causes system failure. Also, subsystem mission time is equal to system mission time. This allocation technique requires expression of reliability requirements in terms of failure rate.

The following steps are followed:

1. The objective is to choose λ_i such that:

$$\sum_{i=1}^{n} \lambda_i \leq \lambda$$

Where: λ_i is the failure rate allocated to subsystem i
λ is the required system failure rate

2. Determine the subsystem failure rates (λ_i) from past observation or estimation.

3. Assign a weighting factor (w_i) to each subsystem according to the failure rates determined in (2) above.

$$w_i = \frac{\lambda i}{\sum_{i=1}^{n} \lambda_i}$$

4. Allocate subsystem failure rate requirements.

$$\lambda_i = w_i \lambda$$

<u>Example</u>: To illustrate this method, consider a system composed of three subsystems with predicted failure rates of $_1 = 0.003$, $_2 = 0.001$, and $_3 = 0.004$ failures per hour, respectively. The system has a mission time of 20 hours and 0.90 reliability is required. Assume that system reliability can be defined by the exponential equation: R=e

Find the subsystem requirements.

The apportioned failure rates and reliability goals are found as follows:

1. $R(20) = \exp[- \lambda (20)] = 0.90$

Then: $\lambda = 0.005$ failures per hour

2. $\lambda_1 = 0.003$, $\lambda_2 = 0.001$, $\lambda_3. = 0.004$

3. $$W_1 = \frac{0.003}{0.003 + 0.001 + 0.004} = 0.375$$

$$W_2 = \frac{0.001}{0.003 + 0.001 + 0.004} = 0.125$$

$$W_3 = \frac{0.004}{0.003 + 0.001 + 0.004} = 0.5$$

4. $\lambda_1 = 0.375(0.005) = 0.001875$

$\lambda_2 = 0.125(0.005) = 0.000625$

$\lambda_3 = 0.5(0.005) = 0.0025$

5. The corresponding allocated subsystem reliability requirements are:

$R_1(20) = \exp[-(0.001875)20] = 0.96$

$R_2(20) = \exp[-(0.000625)20] = 0.99$

$$R_3(20) = \exp[-(0.0025)20] = 0.95$$

Other Allocation Techniques There are a number of more complex techniques which are available for the allocation of reliability requirements to the components of a system. Among these are:

- The Agree technique which considers both the complexity and relative importance of each subsystem.
- The Minimization of Effort technique which considers minimizing the total effort expended to meet the system reliability requirements.
- The Dynamic Programming technique which provides an approach to the reliability allocation with minimum effort expenditure when the subsystem is subject to different effort functions.

RELIABILITY PREDICTION

Objective of Prediction The operational availability achieved by a Naval system depends upon the type of reliability program implemented in the equipment design. The early design phase is the optimum time, from an economic standpoint for evaluating a design, incorporating design modifications, and establishing long-term reliability characteristics. During the design phase, reliability predictions are performed on the system to identify those components which may cause system failure in operational units. Formal reliability prediction is also necessary in the early design phase of a system to determine if it will be capable of achieving operational availability requirements.

Reliability prediction is the process of quantitatively assessing whether a proposed, or actual, equipment/system design will meet a specified reliability requirement. The primary objective of reliability prediction is to provide guidance for engineering and management decisions, based on the assessment of inherent reliability of a given design. Therefore, the real value of the quantitative expression lies in the information conveyed with this value and the information's use. Predictions alone do not contribute to system reliability without additional actions. Predictions constitute decision criteria for selecting courses of action which affect reliability.

Specific objectives of reliability assessment during development are to: (1) provide continuous, up-to-date information concerning the attainment of reliability requirements; (2) identify design weaknesses in sufficient detail so corrective action can be instituted; and (3) provide a reasonable assessment of design reliability prior to production.

The reliability assessment program starts early and continues throughout the life of the equipment. It is important to identify as soon as possible the failure modes of the equipment, progress in meeting certain criteria, and equipment design weaknesses. The sooner these design characteristics are identified, the easier and more cost effective it is to make any necessary adjustments.

During design and development, predictions serve as quantitative guides against which design alternatives can be judged on reliability. The purposes of reliability prediction include: feasibility evaluation, comparison of alternative configurations, identification of potential problems during design review, logistic support planning and cost studies, determination of data deficiencies, trade-off decisions, allocation of requirements, and definition of the baseline for reliability growth and demonstration testing.

Reliability Prediction Procedures In general, there is a hierarchy of reliability prediction techniques available to the designer depending upon two factors: (1) the depth of knowledge of the design; and (2) the availability of historical data on equipment and component part reliabilities. As the system design proceeds from the conceptual phase through development to the production phase, data describing the system design evolves from a qualitative description of systems functions to detailed specifications and drawings suitable for hardware production. A hierarchy of reliability prediction techniques are developed to accommodate the different reliability study and analysis objectives, and the availability of detailed data as the system design progresses.

Basically, the reliability prediction process involves the application of individual component failure rates to the reliability model which was developed and is updated as the design progresses. In general, reliability prediction requires: (1) development of an accurate model of system performance and reliability; and (2) derivation of adequate data to forecast failure frequency for each system component. As described in a preceding section, the system reliability model must replicate the functional performance of the system, based on a description of design engineering parameters. The model must also realistically describe all possible failure modes and their effects on the system. The failure data utilized in the model must be derived from equipment which is similar to the system's mission profile in design characteristics, environmental conditions, and operational use.

Reliability prediction techniques can be classified in five categories, depending on the type of data and information availability for the analysis. The categories are:

1. Similar Equipment Technique The equipment under consideration is compared with similar equipments of known reliability in estimating the probable level or achievable reliability.

2. Similar Complexity Technique The reliability of a new design is estimated as a function of the relative complexity of the subject item with respect to a "typical" item of similar type.

3. Prediction by Functional Technique Previously demonstrated correlations between equipment functions and reliability are considered in obtaining reliability predictions for a new design.

4. Part Count Technique Equipment reliability is estimated as a function of the number of parts in the equipment, in each of several part classes.

5. Stress Analysis Technique The equipment failure rate is determined as a function of all individual part failure rates, considering part type, operational stress level, and derating characteristics of each part.

Another procedure for reliability prediction is the use of a computer program to perform the calculation. Reliability predictions for complex systems frequently require a large amount of tedious computation and a number of "off-the-shelf" software programs have been developed for performing reliability predictions. However, prediction through a computer program utilizes the basic reliability model structure previously described, written in digital program form, and one of the five basic prediction techniques. The Program

Manager should check his computer installation to determine which programs are available or should be obtained before performing any laborious manual calculations.

MIL-STD-756B defines requirements for the application of the basic prediction techniques. In addition, Section 5.1 of MIL-HDBK-217D presents detailed requirements for the application of the Part Stress Analysis Prediction technique, and Section 5.2 presents information on the application of the Parts Count Reliability Prediction method. These specific methods, and the handbook itself, have been developed for analysis of electronic equipment. The Program Manager should be aware of the difficulties inherent in reliability prediction for non-electronic and mechanical equipments.

The most common techniques for prediction of reliability, such as those described in Military Standards and Handbooks, have been developed for analysis of electronic equipment. Therefore, current contractual documentation for Navy equipment usually requires reliability predictions to be determined through methods corresponding to electronic design engineering practices. Reliability prediction is an integral part of the design process and requires coordinated effort between design engineering and reliability engineering activities. In order to be effective, reliability prediction techniques must relate reliability engineering procedures and data to the mission profile and design engineering parameters. Utilization of electronics-oriented procedures for reliability prediction of mechanical systems usually limits the accuracy and usefulness of the quantitative results. The difficulty of reliability prediction for mechanical equipment is the result of several factors inherent to non-electronic technology which increases the complexity of model development and limits opportunities for data collection.

The level of confidence a Program Manager has in a predicted reliability value depends on his level of understanding of the procedures employed in the prediction process. In comparison to the analysis of electronic systems, confidence in reliability predictions for mechanical systems is generally low because a singular, widely accepted approach for mechanical reliability prediction does not exist. The difficulty of establishing standard procedures for mechanical reliability prediction is due, in part, to the complexity of developing realistic models for mechanical systems and the lack of accurate specific failure data on most mechanical equipment.

DESIGN ANALYSIS: FAILURE MODE, EFFECTS AND CRITICALITY ANALYSIS (FMECA)

FMECA Objectives A number of different techniques are available for reliability design analysis to assure the Program Manager that an adequate design evaluation has been conducted, ensuring reliable material will be designed and produced. FMECA is one of these disciplines, and is a structured approach to evaluating the reliability of a design by considering potential failures and the resulting effect on the system. The FMECA is presented as an example of a reliability design analysis technique because it incorporates the procedures described for modeling and predictions. It may also be utilized for analysis of systems maintenance and logistic support.

The procedures of a FMECA are to identify potential design weaknesses through systematic, documented consideration of: all likely ways in which a component or equipment can fail; causes for each mode; and the effects of each failure on the system, which may be different for each mission phase. The primary objective of this design discipline is to iteratively examine all potential failure modes, their causes, and their effects so that the designer will have information on areas where the design may be strengthened.

FMECA should be initiated at the system level as soon as preliminary design information is available. Early identification of all catastrophic and critical failure possibilities allows them to be eliminated or minimized through design correction at the earliest possible time. The FMECA then becomes an iterative process as the design continues through lower levels of development. A properly performed FMECA is invaluable to program decisions regarding the feasibility and adequacy of a design approach. The extent of effort and sophistication of the approach used in a FMECA will be dependent upon the nature and requirements of the program and the system technology. Therefore, it is necessary to tailor the requirements for FMECA to each individual program.

Application of the FMECA The FMECA is a well-documented analysis tool which is utilized for reliability analyses in both defense and commercial industries. Commercial aircraft manufacturers use the FMECA process to certify for the FAA that a new aircraft design is suitable for flight. Under DoD contracts, the FMECA is performed in accordance with MIL-STD-1629A. This standard uses the "tabular" approach to the FMECA process.

The tabular FMECA is the grandfather of all other failure effects analysis techniques. The tabular FMECA employs a simple approach. A table, or worksheet, is used to itemize every probable failure mode and its resulting effect. This analysis is generally referred to as a Failure Mode and Effects Analysis (FMEA). The specific information contained on the worksheet can be tailored to the individual system, but usually includes: item identification, failure mode, probable failure causes, failure effect, method of fault detection, and remarks concerning corrective actions or design changes. Figure D-6 presents the MIL-STD-1629A worksheet for FMEA. The level of detail contained in the analysis is determined by the availability of information and the intended application of the results. The analysis can also include an evaluation of the relative importance of failure modes based upon the severity of their effect on the system and their probability of occurrence. This procedure is called Criticality Analysis (CA), and is also performed in a tabular procedure in MIL-STD-1612A. Figures D-7 and D-8 present the CA worksheet and matrix from the standard. The combined analysis (FMEA and CA) is then referred to as a FMECA. FMECA is a versatile technique which can be used to analyze any system, at any stage in its design.

Basically, the analysis consists of identifying and tabulating the modes by which a system, component or part may fail along with the effect of a failure in this mode. It is performed primarily to isolate and identify weaknesses in the design. FMECA may be applied at any level from complete systems to individual parts. Its purpose is to describe or identify each possible way (the failure mode) an item can fail to perform its function. For a tracking radar, the function of tracking may not be performed due to failure of any of several items, such as the input power, transmitter, receiver, or tracking servo loop. Each single item failure is considered as the only failure in the system while its impacts are analyzed.

Where a single item failure is non-detectable, the analysis is extended to determine the effects of a second failure which, in combination with the first undetectable failure, could result in catastrophic or critical failure condition. Passive and multiple failures which may result in catastrophic or critical conditions are also being identified.

It is important that the Program Manager understands the criticality of scheduling the FMECA. As in most reliability analyses, the FMECA must be performed as early as possible in the systems development in order to be able to impact design reliability. The majority of 72 aerospace firms which responded to a survey by the National Security Industrial Association and the National Aeronautics and Space Administration indicated that they apply a thorough and competent FMECA to new designs, and believe that the analysis

FAILURE MODE AND EFFECTS ANALYSIS

SYSTEM ____________
INDENTURE LEVEL ____________
REFERENCE DRAWING ____________
MISSION ____________

DATE ____________
SHEET ______ OF ______
COMPILED BY ____________
APPFIOVED BY ____________

IDENTIFICATION NUMBER	ITEM/FUNCTION IDENTIFICATION (NOMENCLATURE)	FUNCTION	FAILURE MODES AND CAUSES	MISSION PHASE/ OPERATIONAL MODE	FAILURE EFFECTS			FAILURE DETECTION METHOD	COMPENSATING PROVISIONS	SEVERITY CLASS	REMARKS
					LOCAL EFFECTS	NEXT HIGHER LEVEL	END EFFECTS				

Figure D-6: Example of FMEA Worksheet

608-056

Figure D-6

equipment failure frequency, expressed as Mean Time Between Failure (MTBF).

CRITICALITY ANALYSIS

SYSTEM ____________
INDENTURE LEVEL ____________
REFERENCE DRAWING ____________
MISSION ____________

DATE ____________
SHEET ______ OF ______
COMPILED BY ____________
APPROVED BY ____________

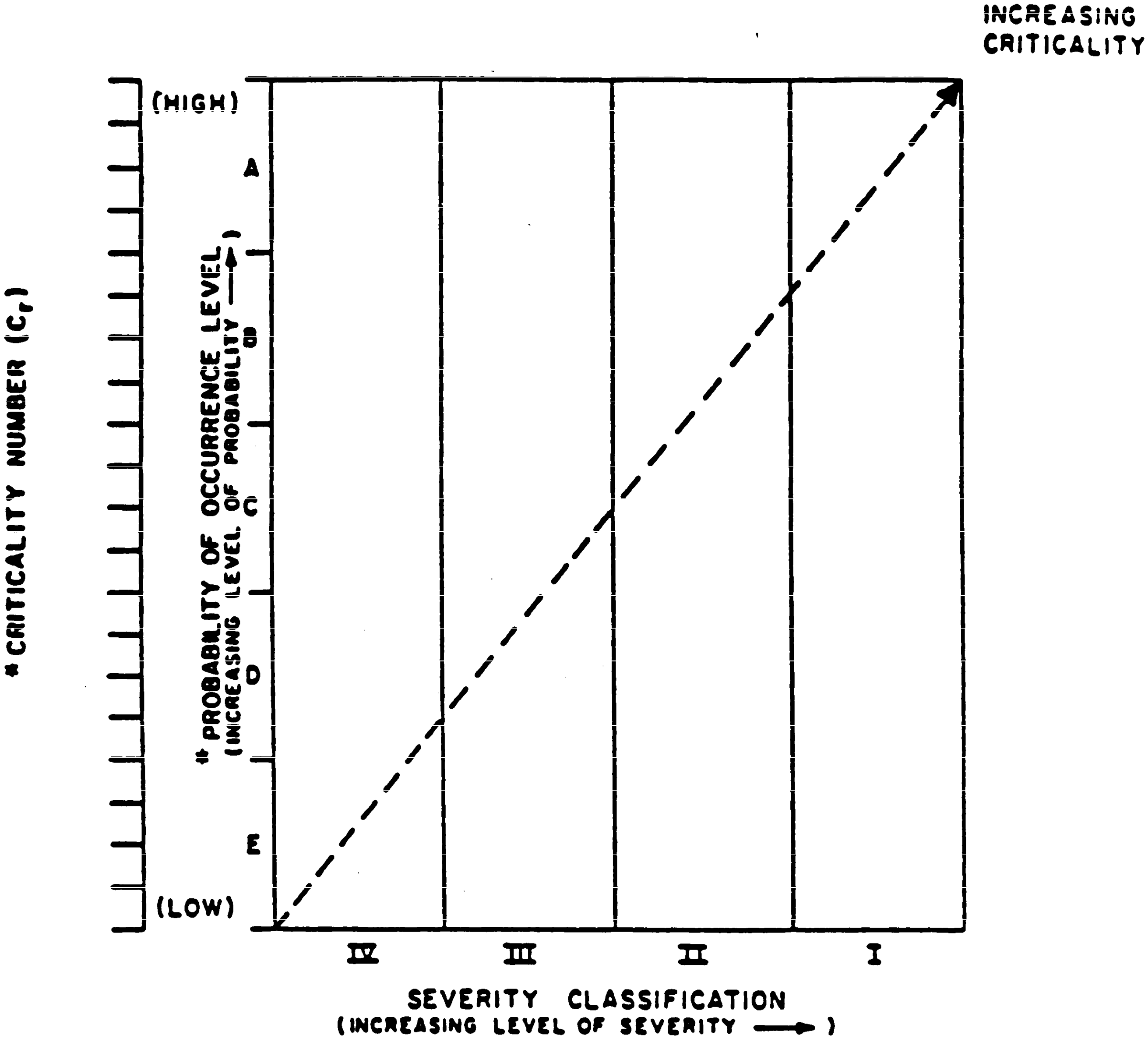
IDENTIFICATION NUMBER	ITEM/FUNCTION IDENTIFICATION (NOMENCLATURE)	FUNCTION	FAILURE MODES AND CAUSES	MISSION PHASE/ OPERATIONAL MODE	SEVERITY CLASS	FAILURE PROBABILITY FAILURE RATE DATA SOURCE	FAILURE EFFECT PROBABILITY (β)	FAILURE MODE RATIO (α)	FAILURE RATE (λ_p)	OPERATING TIME (t)	FAILURE MODE CRIT * $C_m = \beta\alpha\lambda_p t$	ITEM CRIT* $C_r = \Sigma(C_m)$	REMARKS

Figure D-7: Example of a Criticality Analysis Worksheet

804-056

Figure D-7

EXAMPLE OF A CRITICALITY MATRIX



* NOTE: BOTH CRITICALITY NUMBER (C_r) AND PROBABILITY OF OCCURRENCE LEVEL ARE SHOWN FOR CONVENIENCE.

Figure D-8

improved inherent design reliability. However, all firms reported that the FMECA was not effective if it was not performed early in the design process

FMECA Procedures MIL-STD-1629A requires the following basic procedures in performing the FMECA:

1. Define the system to be analyzed A complete system definition includes identification of internal and interface functions, expected performance at all indenture levels, system constraints and failure definitions. Functional narratives of the system should include descriptions of each mission in terms of functions that identify tasks to be performed for each mission, mission phase, and operational mode. Narratives should describe the environmental profiles, expected mission times and equipment utilization, and the functions and outputs of each item.

2. Construct block diagrams Construct functional reliability block diagrams which illustrate the operation, interrelationships and interdependencies of functional entities for each item configuration involved in the system's use. All system interfaces are indicated.

3. Identify Failure modes Identify all potential item and interface modes and define their effects on the immediate function or item, on the system, and on the mission to be performed.

4. Classify failure modes Evaluate each failure mode in terms of the worst potential consequences. Assign a severity classification category.

5. Fault detection and compensation Identify failure detection methods and compensating provisions for each failure mode.

6. Correct design Identify corrective design or other actions required to eliminate the failure or control the risk.

7. Re-evaluate corrective actions Identify effects of corrective actions or other system attributes, such as requirements for logistics support.

8. Document results Document the analysis and summarize the problems which could not be corrected by design. Identify the special controls necessary to reduce failure risk.

These general procedures may be tailored to the individual system under analysis and the specific objectives of the analysis.

MIL-STD-1629A presents five different tasks which can be applied in the FMECA process:

Task 101: Failure Mode and Effects Analysis (FMEA)

Task 102: Criticality Analysis (CA)

Task 103: Maintainability Information

Task 104: Damage Mode and Effects Analysis

Task 105: FMECA

Basic Reliability Design Approaches There are essentially three design approaches or strategies that can be used to satisfy system level reliability requirements: (1) use of highly reliable equipment; (2) graceful degradation; and (3) redundancy. These strategies are limited by several factors including acquisition costs, scheduled manning levels, weight and space, and logistics constraints.

These approaches are listed in the order which would usually be most preferable to the Program Manager. Selection of a highly reliable equipment and parts for the system is usually the most beneficial design approach, but the Program Manager must consider the higher initial cost offset. At the other extreme, use of redundant equipments in parallel is usually the last choice of reliability improvement, due to increased cost and the maintenance/logistic burdens. Each system has unique requirements which drive the Program Manager and the designer towards selection of specific design approaches.

High Reliability Configuration and Component Design The most straightforward design approach that can be used to achieve system reliability requirements is the use of highly reliable equipment or components. No single method can be described for this technique. Basically, this is the application of good design practices to meet an accurate equipment mission profile, with a conservative "safety margin" in selection of equipment stress ratings against anticipated stress levels. The process to achieve this design objective and to assess design status can only be described through the entirety of the reliability engineering discipline. The advantages of this approach include lower support cost, reduced maintenance, reduced spares and weight, and perhaps, reduced initial acquisition cost. Use of high reliability equipments or components is a preferred design approach for achievement of A_O requirements. The drawbacks to this approach are increased development time if the requisite technology is not currently available; increased development costs; and possible risks associated with pushing the state-of-the-art in component manufacturing technology.

System Graceful Degradation The implementation of the latest state-of-the-art design, engineering, and manufacturing procedures and processes cannot guarantee reliability in today's advanced, highly complex weapon systems. To assure the highest reliability and operational readiness, a "building block" approach to system design can be utilized. The basic "blocks" are interconnected so that a malfunction, either equipment failure or battle-damage, will not degrade or inhibit the operation of the total system. This multiple function design approach, redundancy, or "graceful degradation", enhances total system reliability by allowing a minimum number of functions to be performed which permit mission completion.

Graceful degradation is utilized in a system design which employs a network of similar items. Parallel paths within a network are capable of carrying an added load when elements fail. This can result in a degradation to tolerable output. In other words, an element failure in a parallel path does not always cause complete equipment failure, but, instead, degrades equipment performance. The allowable degree of degradation depends on the number of alternate paths available. Where a mission can still be accomplished using an equipment whose output is degraded, the definition of failure can be relaxed to accommodate degradation. Naturally, finite values of degradation must be built into the new definition of failure. This slow approach to failure is exemplified by an array of elements configured into an antenna or an array of detectors configured into a receiver. In either case, individual elements may fail, reducing resolution, but if a minimum number operate, resolution remains great enough to identify a target.

This technique requires application of such design considerations as load sharing, functional modularization, reconfiguration, and selective redundancy. These design considerations achieve basic system performance characteristics with a minimal increase in complexity, providing a payoff in high system reliability.

The heart of the AEGIS Weapon System is the AN/SPY-lA radar. It exemplifies the graceful degradation concept inherent in the total system. The AN/SPY-lA transmitter provides full transmitted power through 32 separate RF power channels. The loss of a channel does not greatly degrade system performance. The online maintenance capability of the radar allows for repairs to be performed by normal maintenance procedures with no system downtime. This feature allows the radar to achieve the required A_o even though a malfunction has occurred.

Graceful degradation is also a feature of the multiple computer system of AEGIS. The three computers, each consisting of four bays, have an automatic reload/reconfiguration ability. If a malfunction or failure involves a computer program error, automatic detection by the executive program initiates a computer decision to automatically reload the program from disc. If there is a hardware failure, the executive program isolates the failure to a bay and automatically reloads a reduced program into the three remaining operational bays. For all computer failures, restoration of system performance may be accomplished in under 15 seconds.

The successful application of this technique requires extensive planning during preliminary design to ensure that interfacing system designs such as air conditioning, power, or compressed air on the larger system are designed to support the graceful degradation. Switching networks can also become complex and expensive. They can make a significant contribution to system unreliability unless they are treated with the same attention as the primary system.

Redundancy The reliability of a system can be significantly enhanced through redundancy. Redundancy involves designing one or more alternate functional paths into the system through addition of parallel elements.

Redundancy has been extensively applied in airborne systems. For example, the electronic multiplexing system for the B-l bomber used a redundant design. In this system, redundant computers control the main switching busses. Normally, one of the two computers is active and feeds the two main busses which control all switching functions, while the other continuously performs the same function and compares its output with the active computer. If the active computer malfunctions, the standby automatically takes over.

Another example of a redundant configuration is provided by the AWG-9 weapon control system used aboard the Grumman F-14 fighter.

In this system, two major sensors are used to achieve the same goal:

1. Pulse doppler search, track, acquisition, and guidance radar.

2. Gimbal-mounted infrared search/acquisition sensor.

The infrared system provides a backup to the radar if the latter is inoperable due to malfunction or jamming. Additionally, it may operate in a dual mode to augment the radar search.

This treatment of redundancy is not meant to be conclusive, but to point out concepts for redundancy important to equipment design applications, and to caution the designer that applications of redundancy have some drawbacks.

General Concepts of Redundancy Mission reliability can be increased through redundancy at the cost of increasing unscheduled maintenance. The unscheduled maintenance increase accompanying redundancy may be offset by improving reliability through use of component improvement techniques, such as parts screening, derating, and design simplification.

Depending on the specific applications, a number of approaches are available to improve reliability through redundant design. These design approaches can be classified on the basis of how the redundant elements are introduced into the system to provide a parallel function path. In general, there are two major classes of redundancy:

1. Active redundancy External components are not required to perform detection, decision, and switching when an element or path in the structure fails.

2. Standby redundancy External elements are required to detect, make a decision, and switch to another element or path as a replacement for a failed element or path.

Techniques related to each of these two classes are depicted in the simplified tree-structure shown in Figure D-9.

Figure D-10 presents the basic redundancy technique based on design configuration. Although not readily apparent, redundancy does not lend itself to categorization exclusively by element complexity. The configurations described in Figure D-10 are more applicable at the part or circuit level as opposed to the equipment level, not because of inherent limitations of the particular configuration but rather to supporting factors such as cost, weight, and complexity.

The decision to use redundant design techniques must be based on a careful analysis of the trade-offs involved. Redundancy may be the only available method when other techniques of improving reliability have been exhausted, or when methods of equipment or part improvement are more costly than duplications. Its use may benefit maintenance planning, since the existence of a redundant equipment can allow for repair without system downtime. Occasionally, there are situations when equipments cannot be maintained, such as satellites. In such cases, redundant elements may prolong operating time significantly.

The application of redundancy has penalties. It will increase weight, space, complexity, cost, and time to design. In general, the reliability gain for additional redundant elements decreases rapidly for additions beyond a few parallel elements. As illustrated by Figure D-11 for simple parallel redundancy, there is a diminishing gain in reliability as the number of redundant elements is increased. As shown for the simple parallel case, the greatest gain achieved through addition of the first redundant elements is equivalent to a 50 percent increase in the system MTBF. In addition to increased maintenance costs for repair of the additional elements, reliability of certain redundant

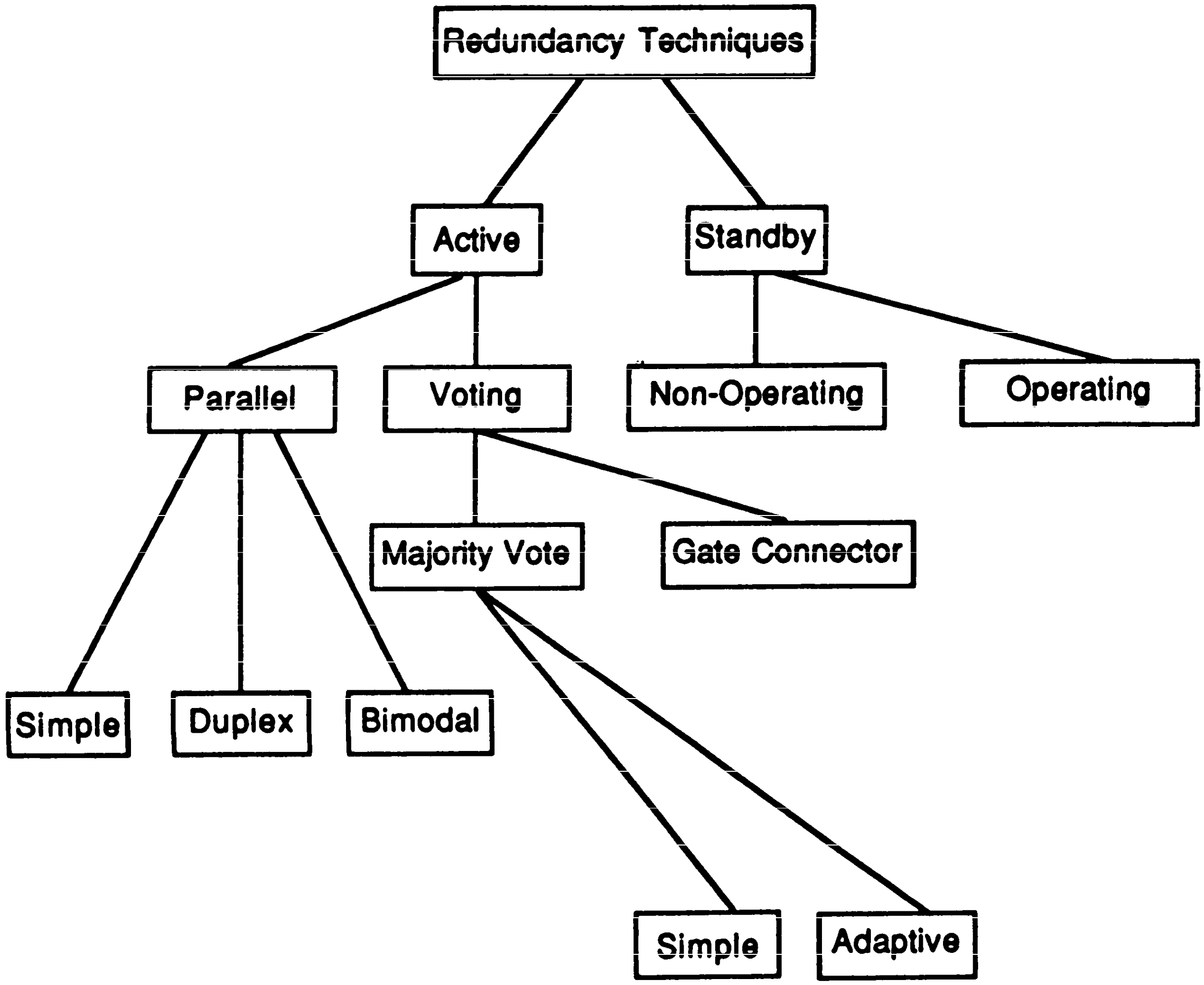


Figure D-9:

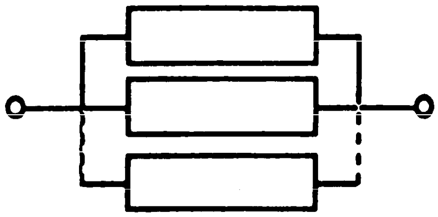
TYPES OF REDUNDANCY

606-024

Continuous-use systems: Systems that are (nearly) always in use during

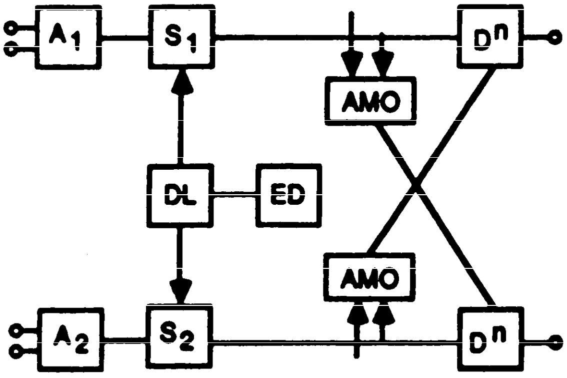
REDUNDANCY TECHNIQUES

Simple Parallel Redundancy



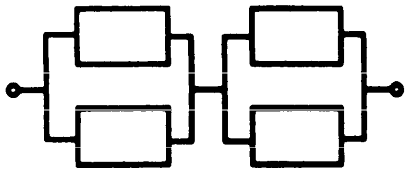
In its simplest terms, redundancy consists of a simple parallel combination of elements. If any element fails open, identical paths exist through parallel redundant elements.

Duplex Redundancy

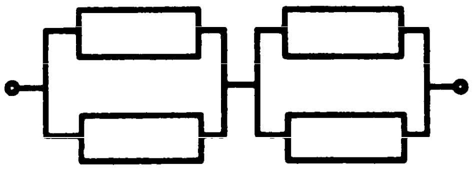


This technique is applied to redundant logic sections, such as A_1 and A_2 operating in parallel. It is primarily used in computer applications where A_1 and A_2 can be used in duplex or active redundant modes or as a separate element. An error detector at the output of each logic section detects noncoincident outputs and starts a diagnostic routine to determine and disable the faulty element.

(a) Bimodal Parallel/ Series Redundancy



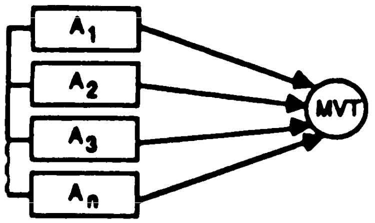
(b) Bimodal Series/ Parallel Redundancy



A series connection of parallel redundant elements provides protection against shorts and opens. Direct short across the network due to a single element shorting is prevented by a redundant element in series. An open across the network is prevented by the parallel element. Network (a) is useful when the primary element failure mode is open. Network (b) is useful when the primary element failure mode is short.

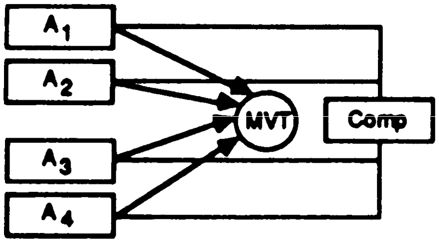
Figure D-10

Majority Voting Redundancy



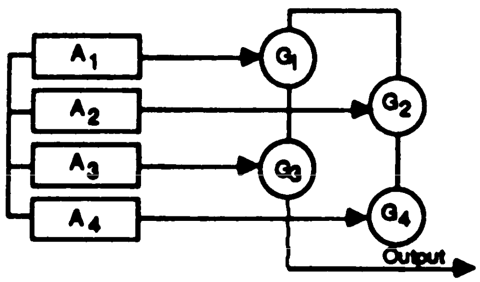
Decision can be built into the basic parallel redundant model by inputting signals from parallel elements into a voter to compare each signal with remaining signals. Valid decisions are made only if the number of useful elements exceeds the failed elements.

Adaptive Majority Logic



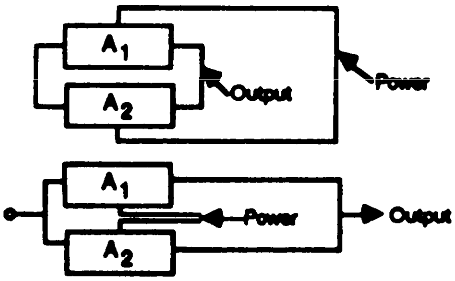
This technique exemplifies the majority logic configuration discussed previously with a compilation and switching network to switch out or inhibit failed redundant elements.

Gate Connector Redundancy



Similar to majority voting. Redundant elements are generally binary circuits. Out puts of the binary elements are fed to switch-like gates which perform the voting function. The gates contain no components whose failure would cause the redundant circuit to fail. Any failures in the gate connector act as though the binary element were at fault.

Standby Redundancy

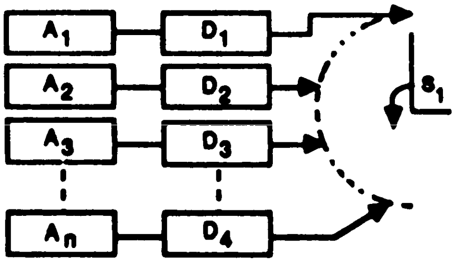


A particular redundant element of a parallel configuration can be switched into an active circuit by connecting outputs of each element to switch poles. Two switching configurations are possible.

1) The element may be isolated by the switch until switching is completed and power aplied to the element in the switching operation.

2) All redundant elements are continuously connected to the circuit and a single redundant eleiment activated by switching power to it.

Operating Redundancy

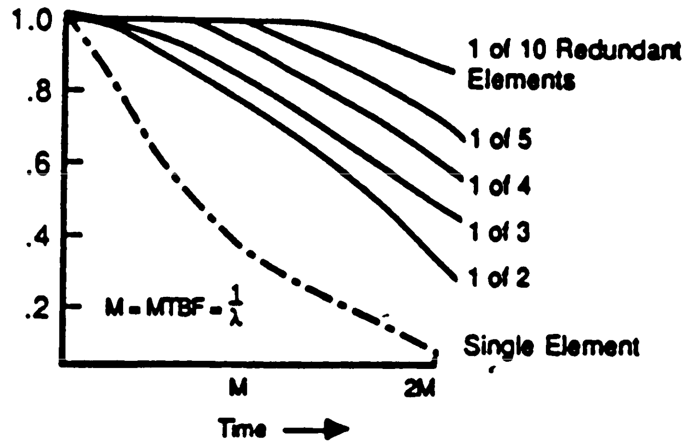


In this application, all redundant units operate simultaneously. A sensor on each unit detects failures. When a unit fails, a switch at the output transfers to the exit and remains there until failure.

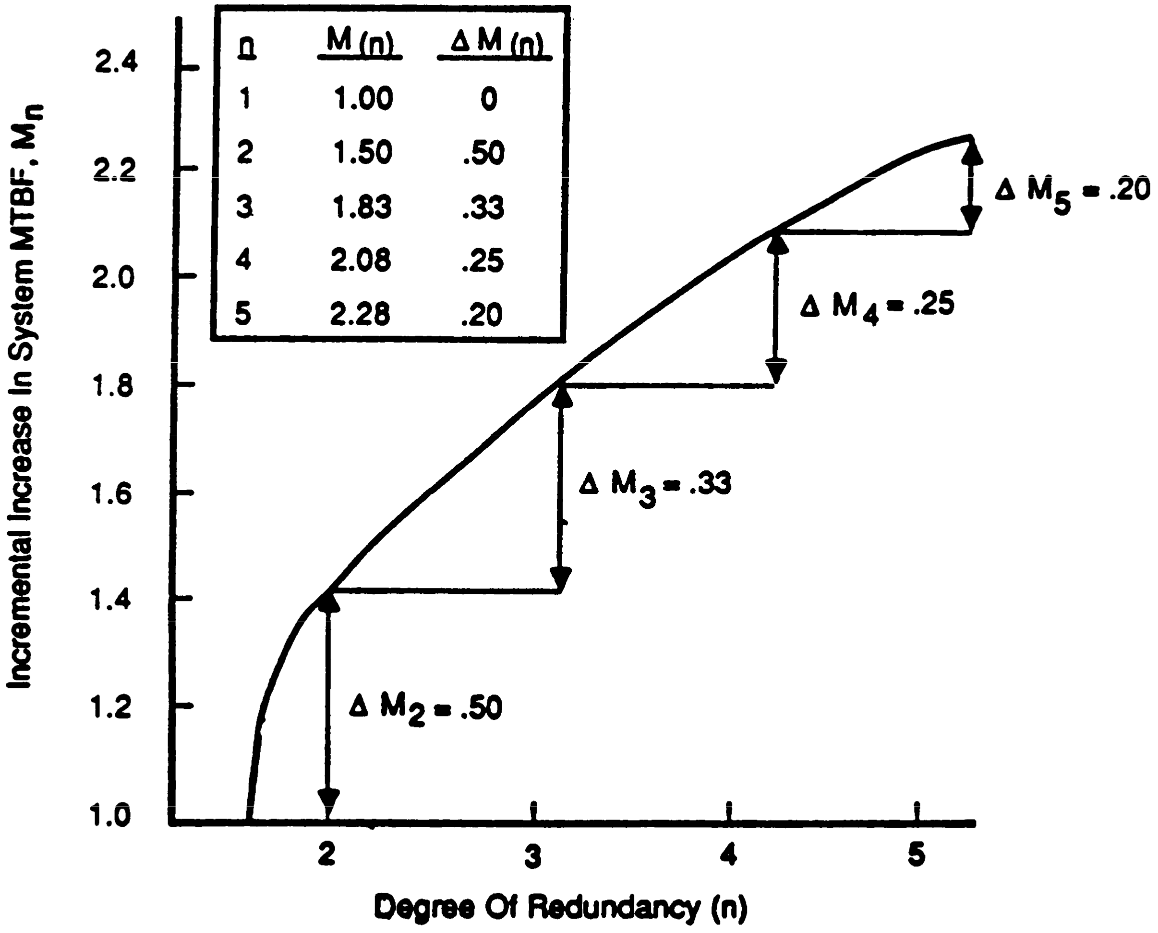
606-071

Figure D-10 (cont.): Redundancy Techniques

DECREASING GAIN IN RELIABILITY



(a) Simple Active Redundancy For One of n Element Required



n	M (n)	Δ M (n)
1	1.00	0
2	1.50	.50
3	1.83	.33
4	2.08	.25
5	2.28	.20

(b) Incremental Increase in System MTBF For n Active Elements

606-064

Figure D-11

configurations may actually be less. This is due to the serial reliability of switching or other peripheral devices needed to implement the particular redundancy configuration (see Figure D-10).

The effectiveness of certain redundancy techniques (especially standby) can be enhanced by repair. Standby redundancy allows repair of the failed unit (while operation of the good unit continues uninterrupted) by virtue of the switching function built into the standby redundant configuration. The switchover function can readily provide an indication that failure has occurred and operation is continuing on the alternate channel. With a positive failure indication, delays in repair are minimized. A further advantage of switching is related to Built-In Test (BIT). BIT can be readily incorporated into a sensing and switchover network for ease of maintenance.

An illustration of the enhancement of redundancy with repair is shown in Figure D-12. The achievement of increased reliability brought about by incorporation of redundancy is dependent on effective isolation of redundant elements. Isolation is necessary to prevent failure effects from adversely impacting other parts of the redundant network. The susceptibility of a particular redundant design to failure propagation may be assessed by application of FMEA. The particular techniques addressed in the previous section on FMECA offer an effective method of identifying likely fault propagation paths.

Interdependency is most successfully achieved through standby redundancy, as represented by configurations classified as decision with switching, where the redundant element is disconnected until a failure is sensed. Design based on such techniques must provide protection against switching transients and consider effects of switching interruptions on system performance.

Furthermore, care must be exercised to assure that reliability gains from redundancy are not offset by increased failure rates due to switching devices, error detectors, and other peripheral devices needed to implement the redundant configurations.

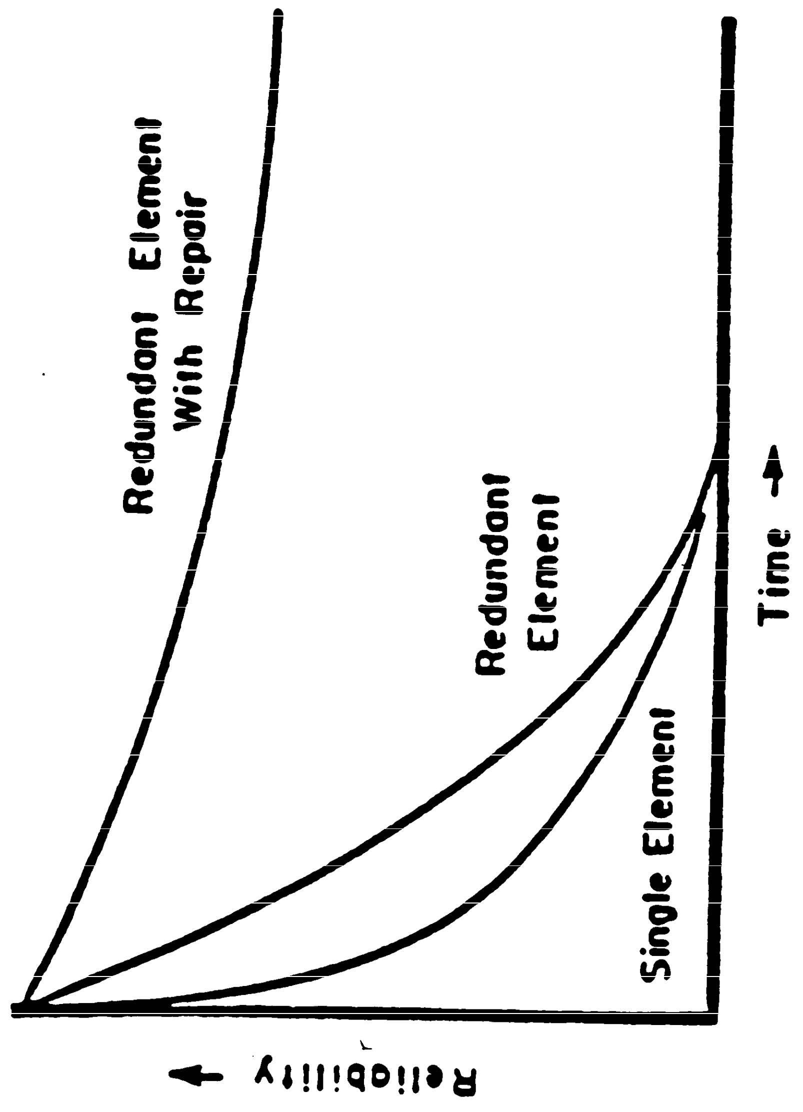


Figure D-12: Reliability Gain for Redundancy with Repair